PDR RID Report

Date Last Modified 5/12/95

Originator Groff, Robert; Isaac David

Phone No 301-901-9236

Organization MITRE

E Mail Address rgroff@mitre.org

Document DID 313 ICD and PDR Presentation Day3

RID ID **PDR** 307

Review CSMS

Originator Ref ICD 1.1

Priority 2

Section Section 3.3 **Page** YS-11 thru YS-19 **Figure Table** Figure or Table

---

Category Name Design-MSS **Actionee** HAIS

Sub Category

Subject SNMP TRAP notification of faults and security violations not sufficient

Description of Problem or Suggestion:

Fault management and security management both depend on the receipt of an SNMP TRAP message from a management agent to identify a fault or a security violation. Because a TRAP message in SNMP is not acknowledged, and SNMP runs over an unreliable protocol (UDP), it is possible that the TRAP sent from the management agent could be lost. In this case the agent would not know that the manager did not receive the TRAP; hence, the manager would never be aware of the fault or the security violation. Section 4.3.1.2 of the ICD specifies that the "management agent service log file captures the event message"; however this does not ensure that there is timely notification of security violations or faults.

Originator's Recommendation

Provide a reliable mechanism notification of security violations or faults in a timely manor.

GSFC Response by: **GSFC Response Date**

HAIS Response by: Forman **HAIS Schedule**

HAIS R. E. Sastry **HAIS Response Date** 5/2/95

SNMP is the communication protocol selected for Release A. Hardware equipment such as routers, hubs and hosts currently use SNMP traps for reporting events. While we agree that SNMP does not have "guaranteed delivery" and that there is a possibility of lost messages, it is an accepted standard with wide spread use. SNMP Traps are not, however, the only mechanism for obtaining status and error messages from network devices as periodic polling will also be used to determine status of managed objects.

For host-based and network-based security events, COTS products with reliable event reporting mechanisms are being investigated. For security events in custom-developed software and fault events associated with ECS managed objects other than hardware equipment, reliable notification mechanisms
(the CSS message passing service) are being investigated. Current activities include detailed definitions of all management and security events which will be reported, classification of these events in terms of criticality, and associated reporting mechanisms required. This information will be provided in the CDR delivery of DID 305, Design Specification.

Status **Closed** **Date Closed** **5/12/95** **Sponsor** **Broder**

****** **Attachment if any** ******
